Goppa codes

13^{th} January 2006

Definition 1. A linear code with parameter $[n, k, d]$ such that $k + d = n + 1$ is called a *maximum distance separable* (MDS) code.

§

Theorem 1. Let C be a linear code over $\mathbf{F}_q$ with parameters $[n, k, d]$. Let G be a generator matrix, and H a parity matrix, for C. Then, the following statements are equivalent.

a. C is an MDS code,
b. every set of $n - k$ columns of H is linearly independent,
c. every set of k columns of G is linearly independent,
d. $C^{\perp}$ is an MDS code.

§

Definition 2. An MDS code C over $\mathbf{F}_q$ is said to be *trivial* if and only if C satisfies one of the following cases.

a. $C = \mathbf{F}_q^n$,
b. C is equivalent to the code generated by $\mathbf{1} = (1, \ldots, 1)$,
c. C is equivalent to the dual of the code generated by $\mathbf{1}$. C is said to be *nontrivial* if it is not trivial.

§

The class of Bose, Chaudhuri and Hocquenghem (BCH) codes is a generalisation of the Hamming codes for multiple-error correction. Binary BCH codes were introduced by A Hocquenghem (1959) and then independently by R C Bose and D K Ray-Chaudhuri (1960). D Gorenstein and N Zierler (1961) generalised the binary BCH codes to q-ary ones. The class of Reed-Solomon (RS) codes is a subclass of BCH codes introduced by I S Reed and G Solomon (1960). Goppa codes, a generalisation of BCH codes introduced by V D Goppa (1970 and 1971), are used also in cryptography some examples of which are the McEliece- and the Niederreiter cryptosystems. The Goppa codes are in turn a subclass of alternant codes, which was introduced by H J Helgert in 1974.

Theorem 2. Let $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ be an arbitrary ordering of the $n = 2^m - 1$ non-zero elements of $\mathbf{F}_{2^m}$. Than a word $\mathbf{c} = \{c_0, \ldots, c_{n-1}\}$ is a code word of BCH code if and only if $\sum_{i=0}^{n-1} c_i \alpha_i^j = 0$, where $j = 1, 2, \ldots, 2t$.

§

Definition 3. A q-ary Reed-Solomon (RS) code is a q-ary BCH code of length $q - 1$ generated by

$$g(x) = \left(x - \alpha^{a+1}\right)\left(x - \alpha^{a+2}\right) \cdots \left(x - \alpha^{a+\delta-1}\right)$$

where α is a primitive element of $\mathbf{F}_q$, $a \geq 0$ and $2 \leq \delta \leq q - 1$.

§

Theorem 3. Reed-Solomon codes are MDS. This means that a q-ary Reed-Solomon code of length $q - 1$ generated by $g(x) = \prod_{i=a+1}^{a+\delta-1}\left(x - \alpha^i\right)$ is a $\{q-1, q-\delta, \delta\}$-cyclic code for any $2 \leq \delta \leq q - 1$.

§

Theorem 4. Let C be a q-ary RS code generated by $g(x) = \prod_{i=1}^{\delta-1}\left(x - \alpha^i\right)$, where $2 \leq \delta \leq q - 1$. Then the extended code $\overline{C}$ is also MDS.

§

Theorem 5. Let α be a primitive element of the finite field $\mathbf{F}_q$. Let $q - 1 \geq \delta \geq 2$. The narrow-sense q-ary RS code with generator polynomial

$$g(x) = (x - \alpha)\left(x - \alpha^2\right) \cdots \left(x - \alpha^{\delta-1}\right)$$

is equal to

$$\left\{\left(f(1), f(\alpha), f((\alpha^2)), \ldots, f\left(\alpha^{q-2}\right)\right) : f(x) \in \mathbf{F}_q[x] \quad \text{and} \quad \deg\left(f(x)\right) < q - \delta\right\}$$

§

Theorem 6. Let α be a primitive element of $\mathbf{F}_q$, and let $q-1 \geq \delta \geq 2$. The matrix

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(q-2)} \\ \vdots & & \vdots & \ddots & \vdots \\ 1 & \alpha^{q-\delta-1} & \alpha^{2(q-\delta-1)} & \cdots & \alpha^{(q-\delta-1)(q-2)} \end{pmatrix}$$

is a generator matrix for the RS code generated by the polynomial

$$g(x) = (x-\alpha)\left(x-\alpha^2\right)\cdots\left(x-\alpha^{\delta-1}\right)$$

§

Definition 4. Let $n \leq q$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, where α_i, $1 \leq i \leq n$, are distinct elements of $\mathbf{F}_q$. Let $\mathbf{v} = (v_1, \ldots, v_n)$, where $v_i \in \mathbf{F}_q^*$ for all $1 \leq i \leq n$. The *generalised Reed-Solomon* code $GRS_k(\alpha, v)$ is defined as

$$\{v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n) : f(x) \in \mathbf{F}_q[x] \quad \text{and} \quad \deg(f(x)) < k \leq n\}$$

.

§

Theorem 7. The dual of the generalised Reed-Solomon code $GRS_k(\alpha, vb)$ over $\mathbf{F}_q$ of length n is $GRS_{n-k}(\alpha, \mathbf{v}')$ for some $\mathbf{v}' \in \left(\mathbf{F}_q^*\right)^n$.

§

Theorem 8.

$$\begin{pmatrix} v_1' & v_2' & \cdots & v_n' \\ v_1'\alpha_1 & v_2'\alpha_2 & \cdots & v_n'\alpha_n \\ v_1'\alpha_1^2 & v_2'\alpha_2^2 & \cdots & v_n'\alpha_n^2 \\ \vdots & & \ddots & \vdots \\ v_1'\alpha_1^{n-k-1} & v_2'\alpha_2^{n-k-1} & \cdots & v_n'\alpha_n^{n-k-1} \end{pmatrix}$$

§

Definition 5. An *alternant* code $A_k(\alpha, \mathbf{v}')$ over the finite field $\mathbf{F}_q$ is the subfield subcode $GRS_k(\alpha, \mathbf{v})|_{\mathbf{F}_q}$, where $GRS_k(\alpha, \mathbf{v})$ is a generalised RS code over $\mathbf{F}_{q^m}$, for some $m \geq 1$.

§

Theorem 9. The alternant code $A_k(\alpha, \mathbf{v}')$ has parameters $[n, k', d]$, where $mk-(m-1)n \leq k' \leq k$ and $d \geq n-k+1$.

§

Theorem 10. The dual of the alternant code $A_k(\alpha, \mathbf{v}')$ is

$$\operatorname*{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}\left(GRS_{n-k}(\alpha, \mathbf{v}')\right)$$

§

Theorem 11. Given any positive integers n, h, δ and m. If

$$\sum_{w=0}^{\delta-1}(q-1)^w \binom{n}{w} < (q^m-1)^{\left\lfloor \frac{n-h}{m} \right\rfloor}$$

then there exists an alternant code $A_k(\alpha, \mathbf{v}')$ over $\mathbf{F}_q$, which is the subfield subcode of a generalised RS code over $\mathbf{F}_{q^m}$, having parameters $\{n, k', d\}$, where $k' \geq h$ and $d \geq \delta$.

§

Definition 6. Let $g(z)$ be a polynomial in $\mathbf{F}_{q^m}[z]$. Let $L = \{\alpha_1, \ldots, \alpha_n\}$ be a subset of $\mathbf{F}_{q^m}$ such that $L \cap \{\text{zeros of}\, g(z)\} = \emptyset$. Let $R_c(z) = \sum_{i=1}^n \frac{c_i}{z-\alpha_i}$ for $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbf{F}_q^n$. Then, the *Goppa code* $\Gamma(L, g)$ is defined as

$$\Gamma(L, g) = \left\{\mathbf{c} \in \mathbf{F}_q^n : R_c(z) \cong 0 \,(\mathrm{mod}\, g(z))\right\}$$

The polynomial $g(z)$ is called the *Goppa polynomial.* The Goppa code $\Gamma(L,g)$ is said to be *irreducible* if $g(z)$ is irreducible.

§

Theorem 14. A word is a code word of the Goppa code, that is to say, $\mathbf{c} \in \Gamma(L,g)$ if and only if

$$\sum_{i=1}^{n} \frac{g(z)-g(\alpha_i)}{z-\alpha_i} g(\alpha_i)^{-1} = 0$$

§

Theorem 13. Given a Goppa polynomial $g(z)$ of degree t and $L = \{\alpha_1, \ldots, \alpha_n\}$, we have $\Gamma(L,g) = \left\{\mathbf{c} \in \mathbf{F}_q^n : \mathbf{c}H^T = \mathbf{0}\right\}$, where

$$H = \begin{pmatrix} g(\alpha_1)^{-1} & \cdots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{1} \\ \vdots & \ddots & \vdots \\ \alpha_1^{t-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{t-1} g(\alpha_n)^{-1} \end{pmatrix}$$

§

Theorem 14. Given a Goppa polynomial $g(z)$ of degree t and $L = \{\alpha_1, \ldots, \alpha_n\}$, the Goppa code $\Gamma(L,g)$ is the alternant code $A_{n-1}(\alpha, \mathbf{v}')$, where $\alpha = (\alpha_1, \ldots, \alpha_n)$ and

$$\mathbf{v}' = \left(g(\alpha_1)^{-1}, \ldots, g(\alpha_n)^{-1}\right)$$

§

Theorem 15. The Goppa code $\Gamma(L,g)$ is $GRS_{n-t}(\alpha, \mathbf{v})|_{\mathbf{F}_q}$, where $\mathbf{v} = (v_1, \ldots, v_n)$ and

$$\frac{v_i = g(\alpha_i)}{\prod_{j \neq i} ((\alpha_i - \alpha_j))}$$

for all $1 \leq i \leq n$.

§

Theorem 16. Given a Goppa polynomial $g(z)$ of degree t and $L = \{\alpha_1, \ldots, \alpha_n\}$, the Goppa code $\Gamma(L,g)$ is a linear code over $\mathbf{F}_q$ with parameters $[n,k,d]$, where $k \geq n - mt$ and $d \geq t+1$.

§

Theorem 17. The dual of the Goppa code $\Gamma(L,g)$ is the trace code $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(GRS_t(\alpha, \mathbf{v}'))$, where $\mathbf{v}' = \left(g(\alpha_1)^{-1}, \ldots, g(\alpha_n)^{-1}\right)$.

§

Theorem 18. Let $q = 2$. Given a polynomial $g(z)$, let $\tilde{g}(z)$ represent the lowest degree perfect square polynomial that is divisible by $g(z)$, and let $\tilde{t}$ the degree of $\tilde{g}(z)$. For a vector $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbf{F}_q^n$ of weight w, where $c_{i_1} = \cdots = c_{i_w} = 1$, let

$$f_c(z) = \prod_{j=1}^{w} \left(z - \alpha_{i_j}\right)$$

The derivative of $f_c(z)$ is

$$f_c'(z) = \sum_{l=1}^{w} \prod_{j \neq l} \left(z - \alpha_{i_j}\right)$$

Then, $\mathbf{c} \in \mathbf{F}_2^n$ belongs to $\Gamma(L,g)$ if and only if $\tilde{g}(z)$ divides $f_c'(z)$. Consequently, the minimum distance d of $\Gamma(L,g)$ satisfies $d \geq \tilde{t}+1$. If $g(z)$ has no multiple root, that is $g(z)$ is a separable polynomial, then $d \geq 2t+1$.

§

Theorem 19. There exists a q-ary Goppa code $\Gamma(L,g)$, where $g(z)$ is an irreducible polynomial in $\mathbf{F}_{q^m}[z]$ of degree t and $L = \mathbf{F}_{q^m}$ of parameters $[q^m, k, d]$ such that $k \geq q^m - mt$, provided that

$$\sum_{w=t+1}^{d-1} \left\lfloor \frac{w-1}{t} \right\rfloor (q-1)^w \binom{q^m}{w} < \frac{1}{t} q^{mt} \left(1 - (t-1) q^{-\frac{mt}{2}}\right)$$

§

Bibliography

R C Bose and D K Ray-Chaudhuri. On a class of error-correcting binary group codes. *Inform. Control.* **3**, 68–79, 1960

Raymond Hill. *A first course in coding theory.* Clarendon, 1986

V D Goppa. A new class of linear error-correcting codes. *Probl. Peredach. Inform.* **6**, 3, 24–30, 1970

V D Goppa. Rational representation of codes and (L,g) codes. *Probl. Peredach. Inform.* **7**, 3, 41–9, 1971

D Gorenstein and N Zierler. A class of cyclic linear error-correcting codes in p^m symbols. *J. Soc. Ind. App. Math.* **9**, 107–214, 1961

H J Helgert. Alternant codes. *Information and Control.* **26**, 369–80, 1974

A Hocquenghem. Codes correcteurs d'erreurs. *Chiffres.* **2**, 147–56, 1959

San Ling and Chaoping Xing. *Coding theory, a first course.* Cambridge University Press, 2004

I S Reed and G Solomon. Polynomial codes over certain finite fields. *J.Soc.Ind. App. Math.* **8**, 300–4, 1960